Internet Engineering Task Force A.Durand
INTERNET-DRAFT SUN Microsystems,inc.
March, 29, 2004 F. Parent
Expires September 28, 2004 Hexago

Requirements for assisted tunneling
<draft-durand-v6ops-assisted-tunneling-requirements-00.txt>

Status of this Memo

Copyright Notice

Abstract

This document defines requirements for a tunnel set-up protocol that could be used by an ISP to jumpstart its IPv6 offering to its customers by providing them IPv6 connectivity without having to upgrade its access network.

1. Goal and Scope of the Document

The v6ops working group has worked on requirements and scenarios for IPv6 deployment by soliciting input from network operators. This work

has identified a need for an "assisted tunneling" mechanism. For example, an ISP starting its IPv6 offering to its customers without upgrading its access network to support IPv6 could use a "tunnel brokering solution" [ISP, section 5.1.] a la [3053]. What has been identified as missing from that RFC is a tunnel set-up protocol.

In an ISP network where IPv4 is dominant, some of the initial IPv6 deployment phases consists of getting a prefix allocation from the RIR, and peering with other IPv6 ISP (or exchange points).

Getting IPv6 connectivity to the customers involves upgrading the access network to support IPv6, which can take a long time and/or be costly. A tunneled infrastructure can be used as a low cost migration path [ISP, section 5.1].

With such an infrastructure, the ISP can connect its customers to its IPv6 network using its production IPv6 address space, thus facilitating migration towards native IPv6 deployment. The IPv6 deployment roadmap for connecting customers becomes:

- assisted tunneling infrastructure to early adopters,
- native IPv6 to customers where economically justified,
- native IPv6 to all customers.

Note that, as the addressing space used during the transition to native remains the same the customer routing, filtering, accounting [ISP, section 5.] stay the same, and there is no need to maintain any kind of relay.

"Assisted tunneling" is used in this document to described a transition mechanism where the parameters to configure a bi-directional tunnel between an end-node (or leaf network) and a router in the core of an ISP are negotiated through a tunnel set-up protocol. Although this negotiation phase can be automated, this remains different from transition mechanisms like 6to4 that is fully automatic or teredo/isatap which, once the IPv4 address of an initial server/router is configured do not involve any further negotiation phase. In particular, the 'authenticated' mode defined in section 5 enable access control to the IPv6 network where the other transion mechanism have to rely on out of band access control.

This document analyze the requirements for such a tunnel set-up protocol. The v6ops WG scenario and evaluation documents for deploying IPv6 within common network environments are used as input to this document.

2. Applicability

Assisted tunneling is applicable in different IPv6 transition scenarios. The focus of this document is to define the requirements

to apply this mechanism in the IPv4 ISP context making the following assumptions:

- ISP is offering IPv6 connectivity to its customers initially using controlled tunneling infrastructure [ISP, 5.1 Steps in Transitioning Customer Connection Networks]

- The customer configuration may be diverse, and not necessarily predictable by the ISP. The following cases must be supported:
  - a single node,
  - a leaf network,
  - using a globally routable IPv4 address,
  - behind a NAT,
  - using dynamic IPv4 address (internally or externally to the NAT)

There are actually two cases where the IPv4 address of the customer tunnel end point can be dynamic, and both must be supported:

- The device used as tunnel end point is using a dynamic IPv4 address provided by the ISP.
- The device used as tunnel end point is located behind a customer owned NAT box that is also acting as a local DHCP server. In that case, the device IPv4 address may change after a reboot.

The scenario where the ISP is providing IPv6 connectivity to non-customers is out of scope of this document.

Althought the main focus of this document is the ISP scenario, assisted tunneling is applicable in all the other scenarios: unmanaged, enterprise and 3GPP.

In unmanaged networks, assisted tunneling is applicable in the case A (a gateway which does not provide IPv6 at all) [UNMANAGED, section 3] and C (a dual-stack gateway connected to an IPv4-only ISP) [UNMANAGED, section 5].

In 3GPP networks, assisted tunneling can be used in the context of dual stack UE connecting to IPv6 nodes through a 3GPP network that only supports IPv4 PDP contexts [3GPP, 3.1].

3. Requirements for Simplicity

The tunnel set-up protocol must be simple to implement and easy to deploy. In particular, it should not depend on any complex, yet to be designed, protocols or infrastructure pieces.

This protocol is a transition mechanism, thus does not need to be perfect. As a matter of fact, making it perfect would be counter productive, at it would first delay its definition, then make its

deployment more cumbersome and, last but not least, diminish the incentives to deploy native IPv6.

4. Requirements for the non-authenticated Mode (initial tryout)

Assisted tunneling can be provided in two different modes, a simple mode, unauthenticated, essentially aimed at tryout, and a more complete mode, authenticated, aimed at production deployment. The tunnel set-up protocol must support both modes, however ISP deploying it may choose to only support one mode of operation.

Assisted tunneling in the non-authenticated mode is defined for simple "plug & play" scenarios. In this mode, the tunnel establishment is triggered through the execution of a simple program, without any pre-configuration or pre-registration required from the end-user.

The tunnel established is "anonymous", the end-user does not provide any authentication to the server. An ISP using the protocol in this mode may be offering a free service and doesn't wish to require any form of registration. This free service can also be used to offer trial IPv6 service limited to the ISP customers by relying on IPv4 access control.

4.1. Address Allocation

This mode is used to provide IPv6 connectivity to a single host. Allocation of an IPv6 address (/128) to the end-node must be supported in this mode. This IPv6 address is "transient" and may change, but one may implement a mechanism to provide IPv6 address stability in this mode (e.g. cookie mechanism).

See section 6.9 for DNS considerations.

4.2. Service Discovery

In order to offer "plug & play", the non-authenticated mode needs to discover the address of the server that will provide the tunnel connectivity. This discovery must be automatic within an ISP network.

4.3. NAT Traversal

Tunneling through IPv4 NAT must be supported. This should be detected during the set-up phase (section 6.)

4.4 Security Threat Analysis

The un-authenticated mode relies on out of band authentication. It essentially offer the IPv6 service to any of its IPv4 customers. This may be regarded as a feature, but deployment of the service with this mode enable must be done carefully. In particular, security considerations must be taken into account.

If ingress filtering is not in place within the access network, a number of DoS attack can happen:

- Customer A can impersonate someone else's IPv4 address during the set-up phase and redirect a tunnel to that IP address. A then can, for example, start a high bandwidth multimedia flow across that tunnel and saturate its victim's uplink.

- Customer A can impersonate a large number of IPv4 addresses and request tunnel of their behalf. That would quickly saturate the ISP tunnel server infrastructure.

If ingress filtering is in place in the core ISP backbone but not in the access network, the potential victims of the above problems will be limited to the ISP's own customers.

If specific filtering is not in place in the ISP core network, another kind of attack can happen. Customers from another ISP could start using its tunneling infrastructure to get free IPv6 connectivity, transforming effectively the ISP into a IPv6 transit provider.

In this mode, IPv4 return routability checks in the set-up phase of the tunnels seems to be a way to avoid some of these problems at the price of an extra round trip.

5. Requirements for the Authenticated Mode

Assisted tunneling in authenticated mode offers the features listed in the non-authenticated mode (section 4), and some extra features documented in this section.

A particular implementation may choose to only implement a subset of those features, but the protocol must be able to negotiate them all.

The authenticated mode is most valuable in a provider network where deployment of IPv6 is done in a more controlled manner. In such networks, ease of debugging, traceability, filtering and so on are important features.

5.1. Address and Prefix Delegation

The authenticated mode must support delegation of a single address or a whole prefix or a combination of both. The length of the IPv6 prefix delegated must be configurable on the server. In this mode, the protocol must be able to support servers willing to offer stable IPv6 prefixes to the authenticated customers.

See section 6.9 for DNS considerations.

5.2. Authentication

A mechanism for easy user registration should be provided. A service provider should be able to use its existing authentication database.

The authentication mechanism supported should be compatible with standardized methods that are generally deployed. Hooks may be provided to facilitate integration with the ISP management infrastructure (e.g. RADIUS for AAA, billing).

In order to assure interoperability, at least one common authentication method must be supported. Other authentication MAY be supported and should be negotiated between the client and server (e.g., SASL [2222]).

note: not clear what should be the mandatory authentication method. Clear text password is out. Digest-MD5 [2831] seems like a good choice.

As in sectoin 4.4, IPv4 return routability checks could help blocking many DoS attack when IPv4 ingress filtering is not performed in the access network.

5.3. NAT Traversal

Tunneling through IPv4 NAT must be supported. This should be detected during the set-up phase (section 6.)

5.4. Accounting

The assisted tunneling should include tools for managing and monitoring the provided service. Such information can be used to plan service capacity (traffic load) or billing information.

Some useful accounting data are (not exhaustive list):

- Tunnel counters (traffic in/out)
- User utilization (tunnel uptime)
- System logging (authentication failures, resource exhaustion, etc.)

The interface used to provide such information can be through SNMP or an AAA protocol (e.g., RADIUS accounting).

6. General Requirements

6.1 Scalability

The tunnel set-up protocol must be scalable.

6.2 Service discovery requirements

The discovery part of the tunnel set-up protocol should be as automatic as possible.

The discovery mechanism must be able to scale for large ISP who cover different geographical areas and/or have a large number of customers.

Customers may very well try to use this tunnel set-up protocol even if their ISP is not offering the service. In this case, without any previous action taken by their ISP, the discovery part of the tunnel set-up protocol must be able to abort immediately and display the customers a message explaining that no service is available.

6.3 NAT Considerations

The assisted tunnel established by the protocol to be designed must work with the existing infrastructure, in particular it must be compatible with the various customer premise equipments available today. This means that, in particular, the tunnels must be able to traverse one or many NAT boxes of different kinds. There is no requirement for any particular NAT traversal technology. However, as NAT traversal usually requires an extra layer of encapsulation, the tunnel set-up protocol must be able to detect automatically the presence of one or more NAT boxes in the path.

6.4 Keep-alive

When a tunnel has to cross a NAT box, the mapping established by the NAT must be preserved as long as the tunnel is in use. This is usually achieved by sending keep alive messages across the tunnel. Also, the same keep alive messages can enable the ISP tunnel end point to perform garbage collection of its resources when tunnels are not in use anymore. To enable those two functionalities, the tunnel set-up protocol must include the transmission of keep-alive messages. A client MAY choose not to send those messages (for example on ISDN type links), but should then expect that the tunnel may be

disconnected at any time by the ISP and be prepared to restart the set-up phase.

6.5 Latency in Set-up Phases

In certain type of networks, keeping tunnels active all the time is not possible or simply too expensive. In those environments, the protocol must be able to set-up tunnels on demand of the IPv6 applications requiring external connectivity.

The tunnel set-up protocol must then have a low enough latency to enable quasi-instant configuration. Latency is usually a function of the number of packet exchanges required, so minimizing this parameter is important.

6.6 Security

The tunnel set-up protocol must not introduce any new vulnerability to the network.

6.7 Traceability

In production environment, traceability is an important consideration. The tunnel set-up protocol must be instrumentable to enable the collection of usage data that can be used, for example, for capacity planning.

6.8 Phase Out

This assisted tunneling mode is only a transition mechanism to enable ISP to jump start IPv6 service without requiring an immediate global upgrade of access networks and instead enabling a progressive roll out. Once IPv6 is available natively in the access network connecting a customer, there is no reason to keep using tunnels. So the tunnel-setup protocol must have a provision to enable the ISP to signal the user to use native IPv6 instead.

6.9 DNS considerations

It should be possible to have the server side of the protocol automatically register the allocated IPv6 address in the DNS system (AAAA and PTR records) using the ISP name space. Nothing specific is required in the protocol to support this. The details can be implementation specific.

If stable prefix delegation is done, it is expected that the DNS delegation of the associated reverse DNS zone will be also stable and

thus can be performed out of band, so there is no requirement to perform this delegation at the tunnel set-up time.

7. Compatibility with other Transition Mechanisms

7.1 TSP

The tunnel set-up protocol is not required to be compatible with TSP or any particular implementation of the tunnel broker model [3053]. Although, a great deal of experience can be drawn from the operation of tunnel brokers currently using the TSP protocol.

7.2 TEREDO

There is a large number of Teredo clients already deployed, the tunnel set-up protocol should explore the avenue of providing a compatibility mode with Teredo, at least in the 'simple' mode described in section 4. However, it may turn out that supporting a compatibility mode with Teredo either requires to change the Teredo specifications and/or implement Teredo on the tunnel server side. In that case, it might be simpler to say that the compatibility mode should be manage on the client side instead of the server side, that is leave it up to the client to use either one of them.

7.3 ISATAP

Similar considerations as Teredo, section 7.2, applies to Isatap. However, as Isatap can not work accross NAT, it is of much less interest in the framework of this document.

8. Security Considerations

The establishment of a tunnel can be compared to Mobile IP technology, where traffic can be redirected to go from one place to another one. So similar threats exists. In particular, when a customer is asking for the set-up of a tunnel ending at IP address X, the ISP should check:

- the customer is allowed to set-up this tunnel, i.e. he "owns" the IPv6 prefix.
- the customer is allowed to terminate the tunnel where he said he would, i.e. he "owns" the IPv4 tunnel endpoint.

The first check is simply an authentication issue. The second may be more complex, but can be omitted if strict ingress filtering is in place in the access network, i.e. the customer is effectively

prevented from sending packet with an IPv4 source address he does not own.

See section 4.4 for specific security consideration in the non-authenticated mode.

9. Author Addresses

Alain Durand
SUN Microsystems, Inc
17 Network circle UMPK17-202
Menlo Park, CA, 94025
USA
Mail: Alain.Durand@sun.com

Florant Parent
Hexago
2875 boul. Laurier, bureau 300
Sainte-Foy, QC G1V 2M2
Canada
Mail: Florent.Parent@hexago.com

10. Normative References

[2119] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

11. Non Normative References

[2831] Leach, P. and C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.

[2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC2222, October 1997.

[3053] A. Durand, P. Fasano, I. Guardini, D. Lento., "IPv6 Tunnel Broker", January 2001.

[ISP] Lind, M., "Scenarios and Analysis for Introducing IPv6 into ISP Networks", draft-ietf-v6ops-isp-scenarios-analysis-01 (work in progress), February 2004.

[UNMANAGED] Huitema, C., "Evaluation of Transition Mechanisms for Unmanaged Networks", draft-ietf-v6ops-unmaneval-01 (work

in progress), February 2004.

[3GPP] J. Wiljakka, "Analysis on IPv6 Transition in 3GPP Networks", draft-ietf-v6ops-3gpp-analysis-09 (work in progress), March 2004.

12. Full Copyright Statement

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.